

SENTRALISASI SINGLE SIGN ON (SSO) DENGAN MENGGUNAKAN ACTIVE DIRECTORY PADA WINDOWS SERVER



**Disusun sebagai salah satu syarat menyelesaikan Program Studi Strata I pada Jurusan
Informatika Fakultas Komunikasi dan Informatika**

Oleh:

AHMAD NUR RIDLO

L 200 120 087

**PROGRAM STUDI INFORMATIKA
FAKULTAS KOMUNIKASI DAN INFORMATIKA
UNIVERSITAS MUHAMMADIYAH SURAKARTA
2016**

HALAMAN PERSETUJUAN

**SENTRALISASI SINGLE SIGN ON (SSO) DENGAN MENGGUNAKAN
ACTIVE DIRECTORY PADA WINDOWS SERVER**

PUBLIKASI ILMIAH

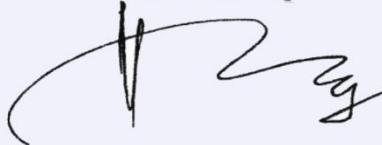
oleh:

AHMAD NUR RIDLO

L 200 120 087

Telah diperiksa dan disetujui untuk diuji oleh:

Dosen Pembimbing

A handwritten signature in black ink, appearing to be 'Bana Handaga', written over a horizontal line.

Dr. Ir. Bana Handaga, M.T.

NIK. 793

HALAMAN PENGESAHAN

**SENTRALISASI SINGLE SIGN ON (SSO) DENGAN MENGGUNAKAN
ACTIVE DIRECTORY PADA WINDOWS SERVER
UNIVERSITAS MUHAMMADIYAH SURAKARTA**

OLEH

AHMAD NUR RIDLO

L 200 120 087

Telah dipertahankan di depan Dewan Penguji
Fakultas Komunikasi dan Informatika
Universitas Muhammadiyah Surakarta
Pada hari Sabtu, 22 Oktober 2016
dan dinyatakan telah memenuhi syarat

Dewan Penguji:

1. Dr. Ir. Bana Handaga, M.T.

(Ketua Dewan Penguji)

2. Helman Muhammad, S.T., M.T

(Anggota I Dewan Penguji)

3. Muhammad Kusban, S.T., M.T

(Anggota II Dewan Penguji)

(.....)
(.....)
(.....)

Publikasi ilmiah ini telah diterima sebagai salah satu persyaratan

Untuk memperoleh gelar sarjana

Tanggal

Mengetahui,

Dekan
Fakultas Komunikasi dan Informatika

Husni Thamrin, S.T., M.T., Ph.D.
NIK : 706

Ketua Program Studi
Informatika

Dr. Hera Suprivono, M.Sc.
NIK:970

PERNYATAAN

Dengan ini saya menyatakan bahwa dalam naskah publikasi ini tidak terdapat karya yang pernah diajukan untuk memperoleh gelar kesarjanaan di suatu perguruan tinggi dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan orang lain, kecuali secara tertulis diacu dalam naskah dan disebutkan dalam daftar pustaka.

Apabila kelak terbukti ada ketidakbenaran dalam pernyataan saya di atas, maka akan saya pertanggungjawabkan sepenuhnya.

Surakarta, 11 Oktober 2016

Penulis

A handwritten signature in black ink, appearing to read 'Ahmad Nur Ridlo', is written over a horizontal line. To the left of the signature is a small, stylized circular mark.

AHMAD NUR RIDLO

L 200 120 087



UNIVERSITAS MUHAMMADIYAH SURAKARTA
FAKULTAS KOMUNIKASI DAN INFORMATIKA
PROGRAM STUDI INFORMATIKA

Jl. A Yani Tromol Pos 1 Pabelan Kartasura Telp. (0271)717417, 719483 Fax (0271) 714448
Surakarta 57102 Indonesia. Web: <http://informatika.ums.ac.id>. Email: informatika@ums.ac.id

SURAT KETERANGAN LULUS PLAGIASI

012/A.3-II.3/INF-FKI/I/2016

Assalamu'alaikum Wr. Wb

Biro Skripsi Program Studi Informatika menerangkan bahwa :

Nama : AHMAD NUR RIDLO
NIM : L200120087
Judul : SENTRALISASI SINGLE SIGN ON (SSO) DENGAN
MENGUNAKAN ACTIVE DIRECTORY PADA WINDOWS
SERVER
Program Studi : Informatika
Status : **Lulus**

Adalah benar-benar sudah lulus pengecekan plagiasi dari Naskah Publikasi Skripsi, dengan menggunakan aplikasi Turnitin.

Demikian surat keterangan ini dibuat agar dipergunakan sebagaimana mestinya.

Wassalamu'alaikum Wr. Wb

Surakarta, 28 Oktober 2016

Biro Skripsi Informatika

Ihsan Cahyo Utomo, S.Kom., M.Kom.



UNIVERSITAS MUHAMMADIYAH SURAKARTA
FAKULTAS KOMUNIKASI DAN INFORMATIKA
PROGRAM STUDI INFORMATIKA

Jl. A Yani Tromol Pos 1 Pabelan Kartasura Telp. (0271)717417, 719483 Fax (0271) 714448
Surakarta 57102 Indonesia. Web: <http://informatika.ums.ac.id>. Email: informatika@ums.ac.id

Turnitin Document Viewer - Google Chrome

https://turnitin.com/dv?s=18o=727517205&u=1057550080&lang=en_us&wisuda%20desember%202016

plagiasi desember - DUE 03-Nov-2016

Originality GradelMark PeerMark

SENTRALISASI SINGLE SIGN ON
BY AHMAD RIDHO

Paper 5 of 14

11% SIMILAR

OUT OF 9

Match Overview

1	Submitted to Universit...	Student paper	6%
2	docslide.us	Internet source	2%
3	eprints.ums.ac.id	Internet source	1%
4	eprints.binadarma.ac.id	Internet source	<1%
5	eprints.binus.ac.id	Internet source	<1%
6	blogs.manageengine.c...	Internet source	<1%
7	etheses.uin-malang.ac.id	Internet source	<1%
8	journal.unpar.ac.id	Internet source	<1%

SENTRALISASI SINGLE SIGN ON (SSO) DENGAN MENGGUNAKAN
ACTIVE DIRECTORY PADA WINDOWS SERVER

Dissusun sebagai salah satu syarat menyelesaikan Program Studi Strata I pada Jurusan
Informatika Fakultas Komunikasi dan Informatika

Okoh:
AHMAD NUR RIDHO
L.200 120 087

PAGE: 1 OF 13

11:40 AM
10/29/2016

SENTRALISASI SINGLE SIGN ON (SSO) DENGAN MENGGUNAKAN ACTIVE DIRECTORY PADA WINDOWS SERVER

UNIVERSITAS MUHAMMADIYAH SURAKARTA

Abstrak

Penelitian ini dilakukan dengan memperhitungkan aspek perkembangan teknologi khususnya pada bidang informasi. Salah satu yang menjadi pusat penelitian adalah sistem *single sign on* (SSO) yang sering digunakan pada aplikasi *web*. Pengelolaan aplikasi *web* dengan jumlah besar sering mengalami permasalahan pada *user* otentifikasi, banyaknya *username* dan *password* yang harus diingat oleh setiap *user* menjadikan efisiensi proses *login* tidak maksimal. Disinilah peran penting dari *single sign on*, dalam mengontrol *user* agar melakukan proses *login* cukup satu kali dan akan otomatis dapat mengakses setiap aplikasi *web* yang terintegrasi di dalamnya. Sistem CAS (Central Authentication Service) atau LDAP (Lightweight Directory Access Protocol) lebih dominan digunakan sebagai pembangunan *single sign on* saat ini. Pada penelitian ini membahas penggunaan *active directory* pada sistem operasi windows server sebagai sentral *single sign on*. Pemanfaatan *active directory* agar mampu bekerja secara optimal sebagai *single sign on* didukung dengan layanan DNS dan Apache Web service. Layanan DNS digunakan sebagai kontrol *domain* dan *subdomain*. Layanan Apache Web service digunakan sebagai kontrol *web page* agar mampu diakses oleh *user*. Pengujian dilakukan dengan cara membuat dua *domain*, sebuah *domain* dan sebuah *subdomain* yang selanjutnya akan diakses oleh *user*. Akses *login* oleh *user* dilakukan terhadap salah satu *domain*, dimana kondisi *user* akan berubah menjadi aktif pada semua aplikasi *web* baik di dalam *domain* maupun *subdomain*. Kendala yang dialami dalam pemanfaatan *active directory* sebagai *single sign on* terletak pada pengaturan *web page* yang harus memiliki data *user* dalam kondisi aktif yang dapat diakses oleh *web page* lain, baik di dalam *domain* maupun pada *subdomain*. Mengatasi permasalahan tersebut digunakan *cookie* sebagai data tersimpan dalam aplikasi *web browser* agar dapat diakses oleh semua *web page* di dalam *domain* maupun *subdomain* dengan syarat masih menggunakan satu aplikasi *web browser* yang sama dan dalam perangkat yang sama. Pengujian sistem terbatas hanya pada jaringan lokal. Hasil yang diperoleh dari pengujian sistem adalah dua puluh *user login* secara bersamaan mampu ditangani oleh *active directory*, jumlah tersebut sesuai dengan perangkat yang tersedia dalam tempat subjek penelitian. Hasil pengujian terhadap performa layanan *active directory* pada penelitian ini menunjukkan adanya jumlah permintaan *user* secara bersamaan dapat ditangani tanpa kegagalan berada pada *range* 10-250 *user*. Sedangkan untuk jumlah permintaan *user* sebanyak 500 terjadi kegagalan sebesar 0,4%.

Kata Kunci: *single sign on*, sso, *active directory*, *domain*, LDAP.

Abstract

This research was conducted by figuring on the development aspect of technology especially in the information field. The big point on this research is the Single Sign On (SSO) system which commonly used in the web application. the web application processing in a large amount is often find a problem in the user authentication, it

caused by too many accounts and passwords which every users should be memorized make the login process efficiency is not maximal. Here is the important role of the sso in controlling user to do the login process only once and it can automatically access all of the integrated web application. Central Authentication Service (CAS) or Lightweight Directory Access Protocol (LDAP) system is more dominant to be used as the development of sso in this present. Furthermore, in this research discusses the usage of the active directory in the windows operating system server as the center of sso. the utilization of active directory to make the optimum capability as sso supported by DNS service and Apache web service. DNS service is used as the domain and subdomain controller. Apache web service is used as the web page controller so it can be accessed by the user. The testing was conducted by making two domains which are domain and sub domain, both will be accessed by the user then. the access login by the user to one of the domains where the user's condition will change into active in whole web application either in domain or subdomain. Problems found in active directory utilization as sso is in webpage setting which need to have the user data in active status and accessible for another webpage either in domain or subdomain. To overcome those problems, cookies as the data stored in the web browser application can be used, to make it accessible for all webpages either in the domain or subdomain with conditions using the same web browser application and device. The system assessment is limited by only using the local network procedure. The result from the system assessment is active directory has a login user capability up to twenty users in the same login time as according to the number of the available devices in the subject research point. The result of the service performance assesment of active directory in this research showed by the amount of the demand from the user in the same than can be handled without failure in range 10 up to 250 users. However, in the amount of 500 users demand found failures 0.4%.

Keyword: single sign on, sso, active directory, domain, LDAP.

1. PENDAHULUAN

Perkembangan teknologi yang pesat berdampak besar terhadap pola hidup manusia. Tidak terkecuali dalam bidang informasi. Keseharian manusia membutuhkan informasi. Dalam memenuhi akan kebutuhan informasi, penyajian informasi menggunakan media elektronik dianggap lebih efektif dan efisien. Jika ditinjau kembali layanan informasi dengan menggunakan media elektronik lebih banyak memanfaatkan aplikasi *web*, dengan penggunaanya yang mudah menjadikan aplikasi *web* sebagai pilihan utama dalam mencari informasi. (Ngafifi 2014).

Layanan informasi digital lebih dominan disajikan dalam bentuk *website*. Dengan memanfaatkan integrasi internet memungkinkan untuk mengumpulkan informasi dari berbagai sumber yang kemudian didistribusikan kepada pengguna. Adanya distribusi informasi maka dibutuhkan kontrol terhadap informasi-informasi tersebut. (Ye 2011).

Pengelolaan aplikasi *web* dikategorikan menjadi *public informations* dan *private informations*. *Public informations* merupakan informasi yang bersifat *universal* dan bebas akses. *Privat informations* merupakan informasi yang bersifat rahasia dan hanya dapat diakses oleh orang yang memiliki hak akses. Dalam penentuan hak akses dibutuhkan pengaturan yang memisahkan antara *user* dan *admin*. Pengaturan hak akses dengan memanfaatkan *active directory* dilakukan pada layanan *user* dan *group*. Dengan pemanfaatan *active directory* sistem keamanan dapat dilakukan untuk menjaga kerahasiaan dari informasi yang bersifat pribadi dengan melakukan otentifikasi *account*. (Suryawan 2014).

Widiharso (2009) dalam jurnalnya yang berjudul “Analisa Implementasi Single Sign On pada Learning Management System dan Internet Protocol Television” menyatakan bahwa layanan LMS dan IPTv yang berdiri sendiri membutuhkan otentifikasi tersendiri agar mampu masuk kedalam sistem. Untuk menangani otentifikasi yang berulang makmadiperlukan implementasi SSO. Penelitian ini terdapat permasalahan dalam melakukan jumlah permintaan layanan. Pada pengujian *respons time* kesimpulan yang didapat adalah semakin lebar *bandwith* jaringan maka semakin cepat *respon* yang dihasilkan. Namun pada pengujian performa dengan seratus permintaan secara bersamaan terjadi *error* sebesar 40% atau setara dengan 40 permintaan gagal pada jaringan terkecil yang diujikan.

Riyanto (2014) dalam skripsinya yang berjudul “Design And Implementation Of SSO (Single Sign On) Using LDAP Authentication For Information System And Hotspot Access At Pesma KH Mas Mansur UMS” menyatakan bahwa salah satu solusi untuk otentifikasi akun adalah menggunakan SSO dengan pemanfaatan LDAP. Proses ini akan mempermudah setiap pengguna karena hanya butuh satu *account* untuk mengakses beberapa sistem seperti sistem informasi Pesma dan hotspot. Dengan pemanfaatan LDAP seluruh data akan terpusat dalam *server* LDAP. Hal ini memungkinkan akan terjadinya beban berlebih pada *server* jika data yang disimpan terlalu banyak. Untuk mengatasi hal tersebut dibutuhkan perangkat yang memiliki kapasitas memori cukup besar agar *delay* yang terjadi dapat diminimalisir. Sistem kerja dari SSO ini adalah melakukan pembacaan data yang berada di dalam *database* dan selanjutnya akan disimpan menjadi satu kesatuan dalam sever LDAP. Kerugian dari sistem tersebut adalah data tidak dapat diakses apabila *server* LDAP mengalami kerusakan. Sedangkan keuntungan dari sistem tersebut adalah adanya penyederhanaan data sehingga memudahkan dalam melakukan manajemen dan pembaharuan data.

Berdasarkan uraian penelitian di atas, penggunaan LDAP dan CAS masih memiliki celah, Maka penggunaan *active directory* dianggap sebagai alternatif yang baik dalam pembangunan SSO. Selain berjalan pada sistem operasi GUI yang mudah dioperasikan, *active*

directory merupakan sistem basisdata yang besar sehingga penggunaannya bersifat *universal* dan digunakan oleh perusahaan berskala besar. Penelitian dengan subjek SDN 1 Pasuruhan Lor Kabupaten Kudus menguarikan latar belakang masalah sebagai berikut, 1) Pemanfaatan teknologi dalam bidang informasi digital yang berupa laporan perkembangan studi, 2) Kebutuhan sistem SSO dalam menangani otentifikasi berulang-ulang terhadap sistem informasi yang dibangun, 3) Pembuatan sistem SSO sederhana yang memanfaatkan *active directory*, 4) Penelitian sebagai studi alternatif penggunaan CAS dan LDAP dalam membangun SSO.

Merujuk pada tinjauan di atas dapat disimpulkan bahwa *single sign on* merupakan salah satu solusi dalam keamanan informasi, dengan memperhatikan aspek jumlah permintaan *user* maka perlu dibangun *server* yang mampu menangani layanan sebanding dengan banyak *user* yang tersedia. Dengan kesimpulan tersebut tujuan dari karya ilmiah ini adalah menerapkan *single sign on* pada proyek yang dikerjakan. Proyek tersebut adalah membuat sistem informasi rapor digital bagi siswa-siswi kelas enam tahun ajaran 2015/2016 yang dapat diakses menggunakan aplikasi *web*. Dalam memenuhi proyek tersebut, sistem keamanan otentifikasi *account* digunakan sebagai pengaman data dan pembatasan hak akses. Sistem keamanan dibangun menggunakan *active directory* yang terdapat pada windows *server* sebagai kontrol *account* terpusat. *Active directory* dipilih dengan mengkategorikan *account* dalam satu sistem sehingga kemudahan manajemen *user* tercapai.

2. METODE PENELITIAN

Penelitian ini menggunakan *active directory* sebagai objek utama, objek pendukung berupa aplikasi *web* sebagai penguji sistem *single sign on* dan mysql sebagai *database* yang dikelola secara terpisah. Penelitian dimulai dengan analisa kebutuhan sistem yang akan dibangun. Tahap selanjtnya pembuatan sistem, dan diakhiri dengan pengujian sistem.

2.1 Analisa Kebutuhan Sistem

Analisa kebutuhan sistem meliputi analisa struktur topologi *active directory*, analisa *single sign on* yang dibutuhkan serta jaringan yang akan digunakan dalam penelitian. Struktur topologi *active directory* dalam penelitian ini merupakan *directory service* yang menyimpan informasi *user account* dan *groups*. Analisa *single sign on* yang dibutuhkan dalam penelitian ini adalah adanya dua level pengguna yakni *administrator* dan *user*. Jaringan yang digunakan dalam penelitian ini terbatas hanya pada jaringan local.

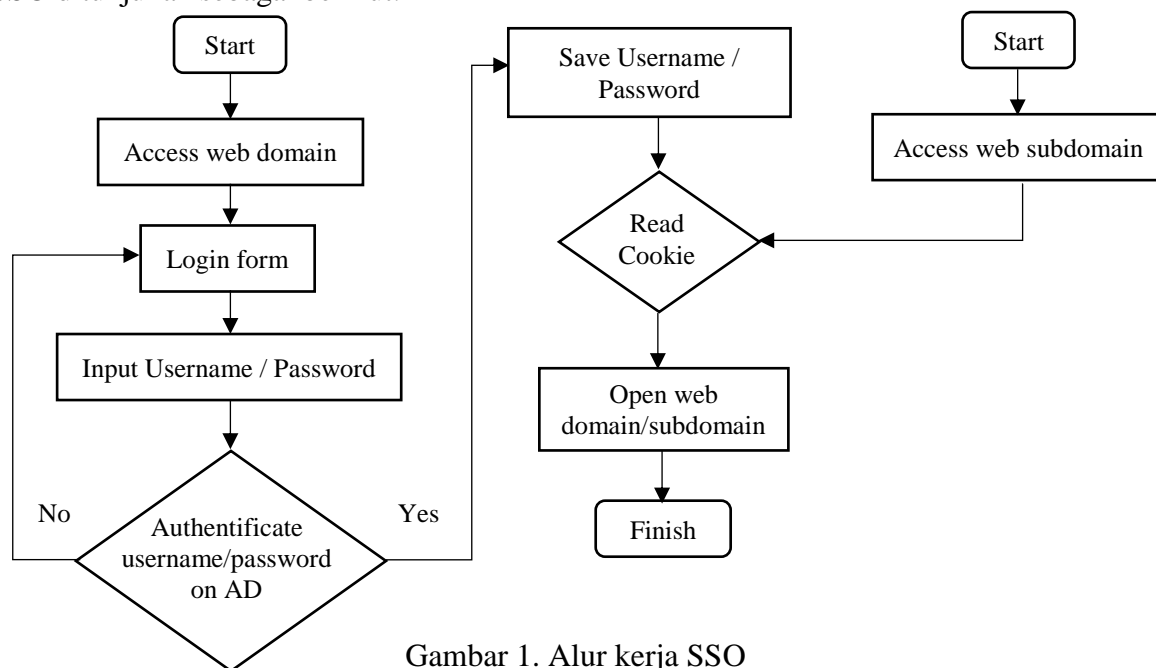
2.2 Perancangan Sistem

2.2.1 Peralatan Utama dan Pendukung

Peralatan utama dan pendukung dalam penelitian ini meliputi perangkat *hardware* berupa laptop ACER Aspire E1-471 dengan spesifikasi utama sebagai berikut, 1) Prosesor Intel Core I-3, 2) Memory RAM 4GB DDR3, 3) Harddisk 500GB. Perangkat *software* yang digunakan meliputi, 1) Windows Server 2008, 2) Windows 10, 3) Virtual Box, 4) Sublime text, 5) XAMPP (Apache/MySQL), 6) Browser Google Chrome.

2.2.2 Algoritma Sistem

Algoritma sistem berisikan tahapan alur kerja dari sistem yang akan dibangun. Algoritma pada SSO ditunjukkan sebagai berikut.



Gambar 1. Alur kerja SSO

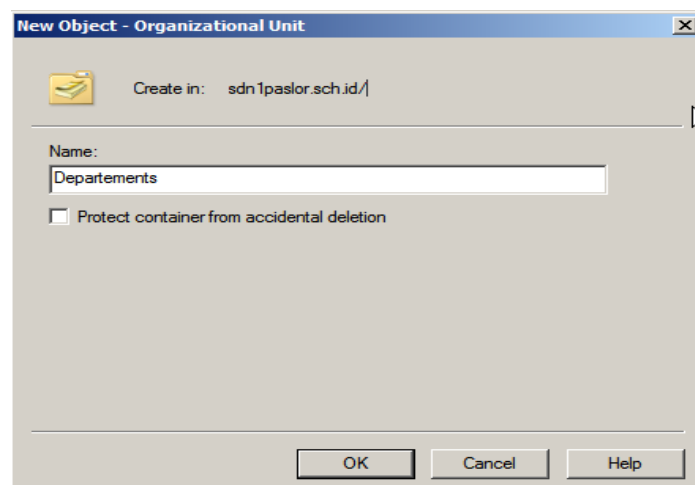
2.3 Implementasi Sistem

2.3.1 Active Directory Domain Services

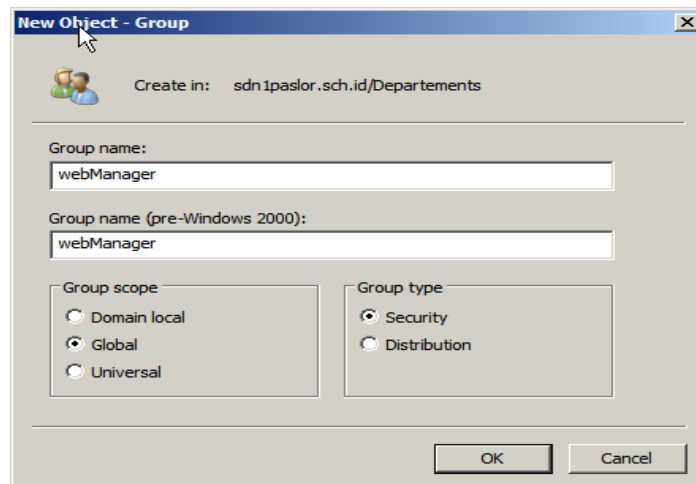
Active directory dibangun dengan melakukan konfigurasi *service* yang ada dalam *server manager*. Agar layanan *active directory* dapat digunakan diperlukan menambahkan *rule* pada sistem. Penambahan *rule* dilakukan dengan memilih menu *add roles* yang terletak dibawah *server manager*.

Selanjutnya akan ditampilkan menu utama berupa tahapan untuk mengaktifkan layanan *active directory* berupa *server roles*, *active directory domain services*, *confirmation*, *progress* dan *result*. Tahapan *server roles* adalah tahap untuk memilih layanan yang akan diaktifkan, pada tahap ini layanan *active directory domain services* akan diaktifkan. Selanjutnya adalah *active directory domain services* dan *confirmation*. Menu *active directory domain services* merupakan informasi dari layanan yang akan diaktifkan meliputi *introduction*, *things to note* dan *additional information*. Menu *confirmation* menunjukkan informasi paket yang akan diaktifkan pada layanan *active directory domain services*.

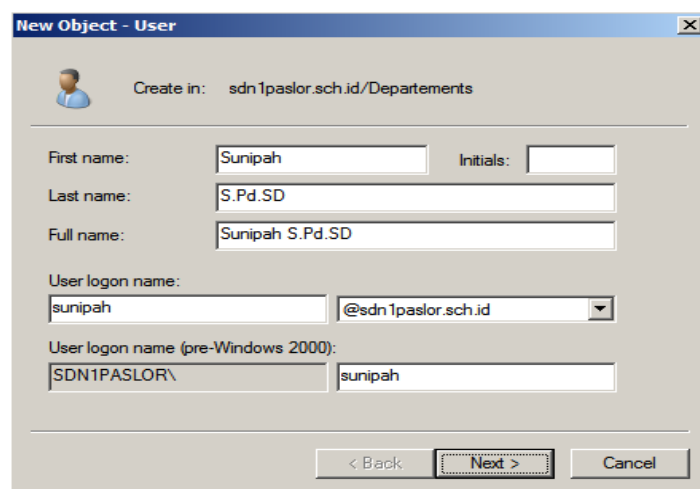
Jika semua layanan telah dikonfirmasi maka proses instalasi akan berjalan yang akan ditunjukkan oleh menu *progress*. Tahap akhir mengaktifkan layanan *active directory* ditunjukkan pada menu *result* sebagai informasi bahwa instalasi telah selesai. Setelah tahap instalasi selesai, tahap berikutnya adalah konfigurasi *active directory* agar dapat digunakan sebagai data *account*. Konfigurasi yang dilakukan meliputi pembuatan *organizational unit*, *group* dan *user account*. Pembuatan *organizational unit* ditujukan agar memudahkan admin dalam pengelompokan divisi yang akan dikelola. Pembuatan *group* dengan tipe *security* ditujukan untuk mengatur perijinan *account* dalam mengakses informasi. Pembuatan *user account* ditujukan untuk mengelola informasi *user* berupa *first name*, *last name*, *initials*, *full name*, *user logon name* dan *password*



Gambar 2. Membuat *organizational unit*, sebagai direktori utama pengelolaan akun



Gambar 3. Membuat *group police* sebagai aturan yang diterapkan ke *user*

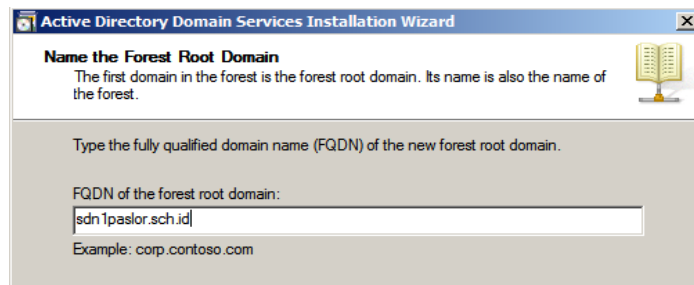


Gambar 4. Membuat *user account*

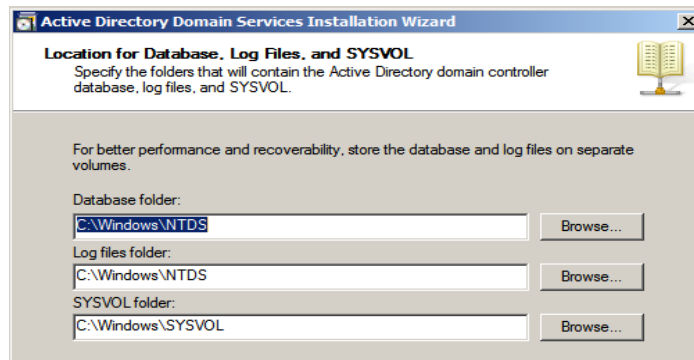
2.3.2 Domain Name Services

Layanan DNS diaktifkan bertujuan menkonfersi alamat IP *server* menjadi alamat berupa nama yang mudah untuk dihafal. Tahap ini akan meminta sejumlah informasi yang akan digunakan untuk sistem *server* berdasarkan *domain* yang dibuat. Informasi yang harus diberikan meliputi *forest root domain*, *forest functional level*, *domain controler*, *database and log file* dan *administrator password*.

Informasi *fores root domain* dimaksudkan untuk memberikan nama alamat IP *server* saat diakses oleh *client*. Sesuai dengan subjek penelitian yang bertempat di SD Negeri 1 Pasuruhan Lor, maka *domain* yang dibuat adalah **sdn1paslor.sch.id**. Informasi *forest funcional level* ditentukan berdasarkan sistem operasi yang digunakan. Informasi *domain controler* adalah layanan dimana *admin* melakukan pengaturan terhadap *domain* yang telah dibuat, pada tahap ini perlu melakukan ceklist layanan DNS *server*. Informasi *database and log file* digunakan sebagai penentuan folder penyimpanan dari data yang akan dikelola. Informasi *administrator password* digunakan sebagai keamanan data yang tersimpan di dalam sistem.



Gambar 5. Mengisi *forest root domain*, sebagai domain *root* pada *server*



Gambar 6. *Database and log file folder*, sebagai lokasi folder pengelolaan data

2.3.3 Apache Service dan Mysql Service

Apache *services* digunakan sebagai penyedia layanan untuk memproses pemrograman dengan menggunakan skrip *hypertext preprocessor* (php). Apache *services* secara *default* bekerja di port 80, sama dengan port yang digunakan *internet information serve* (IIS) yang merupakan layanan pengelola *web* bawaan windows *server*. Adanya kesamaan port yang digunakan menyebabkan layanan tambahan apache tidak dapat berjalan. Pada penelitian ini layanan IIS tidak diaktifkan dan layanan *web* dilakukan sepenuhnya oleh apache. Layanan apache dalam penelitian ini dilakukan dengan menginstal aplikasi XAMPP.

MySQL *services* digunakan sebagai penyedia layanan untuk mengelola rincian data *account*. Untuk mengaktifkan layanan MySQL dapat dilakukan dengan membuka aplikasi *xampp-control panel* dan klik tombol *start* pada layanan MySQL. Data yang dikelola meliputi *profile account* dan nilai siswa kelas 6 sebagai sampel dalam penelitian.

3. HASIL DAN PEMBAHASAN

Sistem SSO pada penelitian ini memanfaatkan *active directory* sebagai pusat otentifikasi *user*. Pada dasarnya jenis layanan SSO ini dapat dikategorikan sebagai bentuk *client server*. *Client server* merupakan arsitektur dimana *client* berfungsi sebagai penerima layanan yang akan menampilkan dan menjalankan *software*. Sedangkan *server* disini bertindak sebagai perangkat yang menyediakan dan mengelola aplikasi, data serta keamanannya. *Active directory* berfungsi sebagai tempat penyimpanan data *account* yang digunakan dalam proses otentifikasi terhadap

web page yang diakses oleh *user*. Dalam penelitian ini *user* melakukan aktifitas *login* pada *web page* yang telah disediakan. Selanjutnya terjadi proses otentifikasi terhadap *username* dan *password* yang dimasukan oleh *user* dengan data *account* yang tersimpan di dalam *active directory*. Proses otentifikasi *user* sukses, selanjutnya terjadi proses pembuatan *cookie*, berfungsi sebagai *regiter* yang tersimpan pada *web browser* dan menunjukkan bahwa *user* berstatus aktif. Setelah tahapan tersebut selesai *user* akan ditunjukan ke *web page* yang dituju serta dapat mengakses *database* yang dibutuhkan. Pada aktifitas selanjutnya dengan kondisi *user* aktif, *user* dapat mengakses *web page* yang berada dalam subdomain tanpa harus melakukan proses pengisian *username* dan *password*. Sistem akan secara otomatis membaca status *account* dan memferikasi terhadap *cookie* yang terdaftar.

Cookie dipilih sebagai salah satu otentifikasi *user* karena relatif mudah untuk digunakan dan mudah untuk dipahami. Berikut adalah *script cookie* yang digunakan dalam penelitian ini.

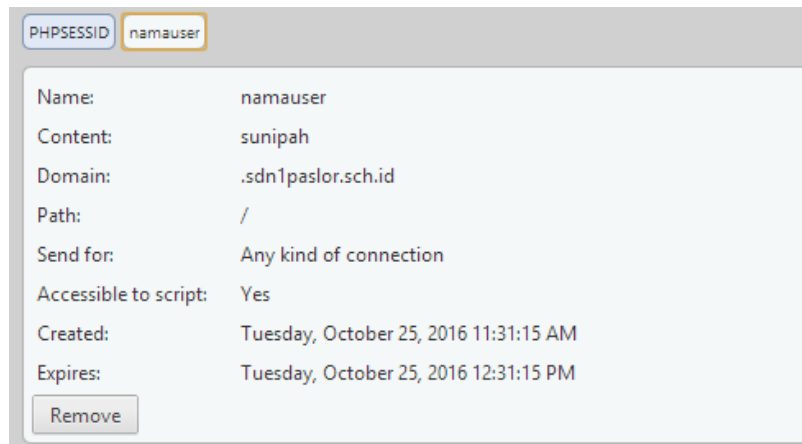
```
setcookie("namauser", $_SESSION[  
    'user'], time()+3600, "/",  
    "sdn1paslor.sch.id");
```

Gambar 7. *Script cookie* tanpa enkripsi

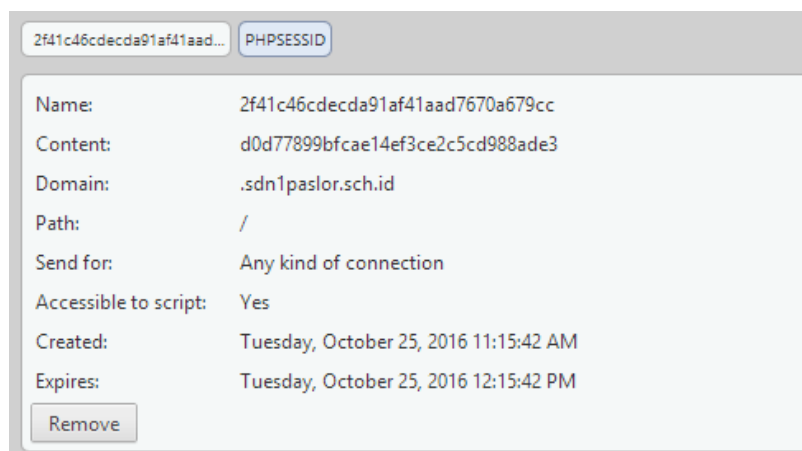
```
setcookie(md5("namauser"),md5($_  
    SESSION['user']), time()+3600  
    , "/", "sdn1paslor.sch.id");
```

Gambar 8. *Script cookie* menggunakan enkripsi

Pada Gambar 7, pembuatan *cookie* dilakukan tanpa melakukan enkripsi sehingga informasi dari *user* yang teregistrasi dapat dibaca oleh pengguna lain dengan mudah. Dengan pertimbangan keamanan maka dibutuhkan enkripsi pada data *cookie* ditunjukan pada Gambar 8. Sehingga informasi yang ditampilkan akan lebih susah terdeteksi. Penjelasan *script* di atas secara singkat sebagai berikut, *setcookie* memlakukan pengesetan paramater, *namauser* paramater nama *cookie* yang tersimpan, *\$_SESSION['user']* paramater nilai dari *cookie* disini merupakan nilai *username* saat *login*, *time()+3600* paramater batas waktu aktif dari *cookie* yang diset, “ / ” paramater dari *path server cookie*, *sdn1paslor.sch.id* paramater yang menunjukkan domain *cookie*, *md5* adalah fungsi enkripsi yang terdapat pada *script php*. Tampilan informasi dari kedua *script* diatas ditunjukan pada Gambar 9. dan Gambar 10.



Gambar 9. Hasil *cookie* tanpa enkripsi



Gambar 10. Hasil *cookie* terenkripsi

Pada Gambar 9. detail informasi *name* dan *content* sangat jelas dan dapat dibaca sedangkan pada Gambar 10. detail informasi *name* dan *content* ditunjukkan dengan kombinasi karakter acak yang kemungkinan untuk dibaca akan lebih sulit. Dengan menggunakan enkripsi informasi *user* lebih terjaga kerahasiannya.

Memanfaatkan jaringan *Local Area Network* (LAN) yang menghubungkan antara *user* dengan *server* SSO. Implentasi jumlah maksimal layanan sebanyak dua puluh *user* dalam satu waktu *login* secara bersamaan. Dalam jaringan ini dilakukan konfigurasi IP secara *static*. Hal tersebut ditentukan dengan pertimbangan jumlah *client* yang relatif sedikit dan beban layanan yang terhadap *server*. Konfigurasi IP memberikan pengaruh pada kecepatan pengiriman data dan kegagalan pengiriman data. Berikut perbandingan data analisa penggunaan DHCP dengan IP *static*.

Tabel 1. Perbandingan DHCP dengan IP Static

Pengujian ke-	DHCP				IP Static			
	Packets			Round- trip (ms)	Packets			Round- trip (ms)
	Sent (unit)	Received (unit)	Lost (%)		Sent (unit)	Received (unit)	Lost (%)	
1	4	4	0	83	4	4	0	0,114
2	4	4	0	64	4	4	0	0,112
3	4	4	0	93	4	4	0	0,112
4	4	3	25	139	4	4	0	0,111
5	4	4	0	67	4	4	0	0,112

Berdasarkan data statistik di atas kecepatan pengiriman data lebih stabil jika menggunakan IP *static*, hal tersebut dilihat dari hasil *round-trip* IP *static* yang perubahannya tidak signifikan dengan menunjukkan nilai *round-trip* terendah sebesar 0,112ms dan nilai tertinggi sebesar 0,114ms. Sedangkan pada hasil *round-trip* DHCP menunjukkan adanya perbedaan yang signifikan, dimana nilai terendah adalah 64ms dan nilai tertinggi 139ms. Perbandingan analisa pada layanan pengiriman data menghasilkan, IP *static* memiliki performa yang lebih baik, dengan lima sampel dalam tabel menunjukkan hasil *received* sukses sebesar 100% dan hasil kegagalan sebesar 0%. Pada analisa layanan pengiriman data menggunakan DHCP dari lima sampel yang ada terjadi kegagalan sebesar 25% yang ditunjukkan pada pengujian sampel ke-4. Berdasarkan hasil tersebut performa dengan menggunakan IP *static* lebih baik dibandingkan dengan DHCP. Hal tersebut dipengaruhi oleh sistem kerja layanan DHCP yang mewajibkan PC *client* melakukan *request* IP terlebih dahulu sebelum melakukan layanan informasi yang lain. Pada IP *static* memungkinkan PC *client* tidak melakukan *request* IP karena telah dikonfigurasi secara manual, sehingga mampu melakukan proses layanan informasi lebih cepat.

Untuk mengetahui kemampuan *server* SSO dalam menangani jumlah layanan secara masal, penulis melakukan *load test* menggunakan software bantu *apache benchmark*. Terdapat dua kategori dalam melakukan *load test*, yaitu uji *respon times* dan uji performa. Uji *respon times* didasari oleh kemampuan *server* SSO *active directory* dalam seberapa cepat melayani permintaan oleh *user* secara bersamaan. Uji performa ditujukan untuk mengetahui persentase sukses *login user* secara masal.

Tabel 2. Pengujian *time respons* (a) dan Pengujian performa (b)

(a)			(b)				
Pengujian ke-	Waktu delay (s)	Jumlah permintaan	Pengujian ke-	Jumlah user	Total waktu proses (s)	Status gagal (%)	Jumlah user gagal
1	1	1.347	1	10	0,000	0	0
2	2	2.752	2	20	0,016	0	0
3	3	4.086	3	50	0,047	0	0
4	4	5.384	4	100	0,078	0	0
5	5	6.143	5	250	0,250	0	0
6	6	8.186	6	500	3,334	0,40	2
7	7	9.303	7	750	8,453	0,67	5
8	8	10.140	8	1000	13,172	0,70	7
9	9	11.657	9	1250	15,891	0,72	9
10	10	13.258	10	1400	18,422	0,72	10

Data pengujian *time respons* di atas, kemampuan *server* dalam melayani permintaan akan semakin meningkat sesuai dengan besar waktu *delay* yang diberikan. Nilai kelipatan dari jumlah permintaan tidak selalu konstan, tetapi perbedaan yang dihasilkan tidak terlampaui signifikan. Hal tersebut dipengaruhi dari seberapa sibuk *traffic* dari *server SSO active directory*. Berdasarkan uraian tersebut disimpulkan besar jumlah permintaan berbanding lurus dengan besar waktu tunda.

Data pengujian performa menunjukkan jumlah permintaan *user* secara bersamaan dapat ditangani tanpa kegagalan berada pada range 10-250 *user*. Sedangkan untuk jumlah permintaan *user* sebanyak 500 terjadi kegagalan sebesar 0,4%, untuk jumlah permintaan *user* sebanyak 750 terjadi kegagalan sebesar 0,67%, untuk jumlah permintaan *user* sebanyak 1000 terjadi kegagalan sebesar 0,7%, untuk jumlah permintaan *user* sebanyak 1250 terjadi kegagalan sebesar 0,72% dan untuk jumlah permintaan *user* sebanyak 1400 terjadi kegagalan sebesar 0,72%, dengan masing-masing jumlah kegagalan yang meningkat. Pada pengujian dengan jumlah *user* lebih dari 1400 terjadi jumlah kegagalan lebih dari 10 *user* dan menyebabkan berhentinya sistem pengujian secara paksa. Sehingga dapat ditarik kesimpulan bahwa kemampuan *server SSO active directory* dapat melayani *user* tanpa adanya kegagalan berada dibawah nilai 500 *user*, dan semakin banyak nilai permintaan dari *user* maka jumlah kegagalan akan semakin meningkat.

4. PENUTUP

Berdasarkan penelitian yang telah dilakukan dapat ditarik kesimpulan bahwa *system single sign on* menggunakan *active directory* pada *windows server* mampu mengatasi otentifikasi login serta menghindari adanya otentifikasi berulang. Penggunaan *cookie* sebagai paramater *account* berstatus aktif dapat berjalan dan berfungsi sebagai acuan dalam membaca *database account*. Pada pengujian performa dalam penelitian ini, diperoleh hasil *respon times* dimana semakin besar waktu tunda maka semakin besar jumlah permintaan yang dapat dilayani, sedangkan *respon requests* yang mampu dilayani secara bersamaan tanpa kegagalan adalah dibawah 500 *user*. Secara teori *active directory* merupakan layanan *database* yang besar dan handal. Adapun kelemahan yang terjadi pada penelitian ini dipengaruhi oleh sistem yang berjalan menggunakan *software* bantu berupa *virtualbox* dan perangkat *hardware* yang minimalis sehingga performa dari *server* tidak berfungsi secara optimal.

DAFTAR PUSTAKA

- Ngafifi, M. (2014). Kemajuan Teknologi dan Pola Hidup Manusia dalam Perspektif Sosial Budaya. *IPI*, Volume 2, No. 1, 2014.
- Widiharso, R. (2009). Analisa Implementasi Single Sign On pada Learning Management System dan Internet Protocol Televion. *Skripsi*. Institut Teknologi Sepuluh Nopember.
- Ye, X., & Zhong, L. (2011). Improving Web Service Security and Privacy. *2011 IEEE World Congress on Services*. doi:10.1109/services.2011.109
- Muliadi Kerta, J. (2011). Penggunaan Single Sign On (SSO) pada Jaringan Internet Badan Pengkajian dan Penerapan Teknologi (BPPT). *Skripsi*, Volume 2 No. 02 December 2011.
- Ramadhan, G. (2013). Analisis teknologi Single Sign On (SSO) dengan penerapan Central Authentication Service (CAS) pada Universitas Bina Darma. *Bina Darma e-Journal*, Vol. XX No.X Oktober 2013: 1-13.
- Grag, P. (2016). SSO (Single Sign On) Implementation. *International Journal of Sicence and Research (IJSR)*, Volume 5 Issue 6, June 2016.
- Kurniawan, F., Fajar, S., & Umi, F. (2014). Membangun Privileges Pada Jaringan Komputer Sma Negeri 2 Boyolali Berbasis Active Directory Dengan Windows Server 2008 Enterprise. *Emitor*, Volume 14 No. 1, Maret 2014.
- Riyanto, A. (2014). Design And Implementation Of SSO (Single Sign On) Using Ldap Authentication For Information System And Hotspot Access At Pesma KH Mas Mansur UMS. *Skripsi*, Informatics Engineering Department UMS.